

ARTICLE APPEARED
ON PAGE A1

WASHINGTON POST
27 May 1986

U.S. Seeking to Limit Access Of Soviets to Computer Data

By Michael Schrage
Washington Post Staff Writer

The Pentagon, concerned about the flow of high technology to the Soviet bloc, is trying to limit foreign access to government and commercial computer data bases that contain sensitive technical information.

A range of legal and technological options are now under exploration, from licensing access to high-tech data bases to planting special computer programs within the data bases to monitor who is seeking what information.

Government officials concede, however, that they face formidable obstacles in devising a workable system, including such questions as whether data bases enjoy the same constitutional protections as other media and how to implement restrictions in ways that won't deny data-base benefits to American users.

"It's a supercomplex problem but it's being worked very intently," said Donald C. Latham, assistant secretary of defense for communications, command, control and intelligence.

The effort stems from a growing perception in the defense community that the export of high-technology data should be as strictly controlled as the export of high-technology goods.

"Cocom [the Coordinating Committee on Multilateral Export Controls, the multinational organization that determines what technologies are subject to export controls] is only beginning to talk about controlling soft information as opposed to hardware," said Stephen D. Bryen, deputy undersecretary of defense for trade security policy.

But Bryen acknowledged that proliferation of global computer networks and legal constraints could make enforcement of restrictions on international data flows very difficult.

Soviet scientists have publicly confirmed that they regularly gain access to U.S. computer data bases through overseas telephone hook-

ups to keep up to date with advances in key technologies plus useful software that often resides in such systems.

At a conference held recently in Rome, the head of the Soviet Union's National Center for Automated Data Exchange indicated that Soviet researchers used data networks in Canada, Europe and elsewhere to gain access to commercial and government data bases in the United States.

These data-base systems, employing sophisticated computer software, enable users to retrieve in seconds reams of important technical data that would otherwise take months of painstaking library research. Data-base retrieval has become an indispensable tool of the international research community.

These systems, ranging from data bases housed in the national laboratories to commercial offerings from companies such as Dialog Inc. and Mead Data Central's Nexis, provide data from such fields as biotechnology, electrical engineering, materials science and high energy particle physics, as well as access to useful computer software.

An Air Force study on the issue, scheduled for release next month, is expected to identify foreign data-base access as a significant defense concern.

At this time, such Soviet bloc data-base retrieval violates no laws, which has prompted the national security community to consider countermeasures.

One approach is to create a new classification of technical data to put it beyond the reach of ordinary data-base access. The National Telecommunications Information Systems Security Committee (NTISSIC), an interagency group chaired by Latham, is expected to recommend the creation of a category of data—called "sensitive"—for federal agencies to implement. These data, defined as potentially related to national security, would require a special password or other method for data-base access.

"The practical option is to consider classification of the data base," said the Defense Department's Bryen.

Another approach is to regulate the export of technical data in much the same way that technical products are regulated. Part 379 of the Export Administration Act could allow the government to license the export of certain kinds of technical information, like computer software.

"The idea is to sharpen that up," said Bryen,

U.S. GOVERNMENT PRINTING OFFICE: 1985

and possibly require foreigners to have a license to use U.S. data bases.

Such actions would raise important legal questions.

While data bases may contain information in the public domain, the ability to use software to search through and organize that data in certain ways "could create information that could rise to the stature of proprietary or 'controlled' information," said Donald Weadon, a Washington attorney specializing in export control law.

"These technical improvements are creating a tension between what has been U.S. policy promoting the free flow of scientific information and the need for sensible controls on the export and dissemination of proprietary technology information with national security implications," he said.

"I'm not aware of this initiative," said Roger Summit, president of Dialog Inc., a major commercial data-base supplier with more than 250 data bases and 80,000 customers, many from overseas. "I don't know under what authority it would be implemented."

"Our clients are confidential, and that is an important policy," said Gerald Yung, general counsel to Mead Data Central, the company that runs the Nexis data base. "We would be sensitive to national security requests; there may be con-

cerns on national security questions—but we know of no such inquiries or concerns on that . . . at this point."

"We recognize that there are legitimate national security concerns," Kenneth B. Allen, vice president, government relations, for the Information Industries Association, a trade organization representing leading commercial data-base suppliers. "But we think it is dangerous for the government to censor or restrict the flow of information. The association is just now starting to grapple with that issue. We're just looking at the opening salvos here."

The Reagan administration has already taken steps to deny foreign nationals access to high-technology data. The Pentagon recently ruled that Soviet scientists should not be allowed to use supercomputers in this country.

"The presumption is that [access to a] supercomputer is the same as if you exported the supercomputer," said Bryen. "Any computer that can't be exported, they shouldn't have access to."

Consequently, Bryen argues, foreign access to data bases stored on powerful computers is tantamount to exporting the power of that computer without an export license.

"What you have to do is make access to data bases a licensable action," he said. But there are legal questions to be resolved before that is possible.

For example, "access to information may not necessarily be licensable at all" under current law, Bryen said, even though it is an option that should be considered.

Another approach is to use technology to monitor data-base access by putting in a computer program that tracks who is seeking access to particular information. For example, a researcher doing a data-base search using such keywords as "defense electronics" and "phased-array radar" might trigger software designed to monitor such inquiries.

"I'm very concerned about what people are doing—and not just the Soviets," said Latham, the assistant defense secretary. "If that means putting a monitor on Nexis-type systems, then I'm for it. The question is, how do you do that technically without unnecessary interference?"